

HOPF ALGEBRAS WITH TRIALITY

GEORGIA BENKART, SARA MADARIAGA, AND JOSÉ M. PÉREZ-IZQUIERDO

ABSTRACT. In this paper we revisit and extend the constructions of Glauber-
man and Doro on groups with triality and Moufang loops to Hopf algebras.
We prove that the universal enveloping algebra of any Lie algebra with triality
is a Hopf algebra with triality. This allows us to give a new construction of
the universal enveloping algebras of Malcev algebras. Our work relies on the
approach of Grishkov and Zavarnitsine to groups with triality.

1. INTRODUCTION

Recall that a *loop* (Q, \cdot, e) is a set with a binary operation $\cdot: Q \times Q \rightarrow Q$ $(a, b) \mapsto ab$ and a unit element $e \in Q$, i.e. $ea = a = ae$ for any $a \in Q$, such that the multiplication operators $L_a: b \mapsto ab$ and $R_b: a \mapsto ab$ are bijective for any $a, b \in Q$ [1, 15]. Roughly speaking a loop is a nonassociative group, or more precisely a group is a loop that in addition satisfies the associative law $(xy)z = x(yz)$.

In the nonassociative setting other loops apart from groups are of interest. One of them is the seven dimensional sphere of octonions of norm 1. This sphere has no structure of a Lie group, however with the product inherited from the octonions, it satisfies the (left, middle and right) *Moufang identities*

$$a(x(ay)) = ((ax)a)y, \quad (a(xy))a = (ax)(ya) \quad \text{and} \quad ((xa)y)a = x(a(ya))$$

for any $a, x, y \in Q$, so in some sense this product is nearly associative. Loops that satisfy any of these identities also satisfy the others, and they are called *Moufang loops*.

To any loop Q is attached the group generated by the multiplication operators $\{L_a, R_a \mid a \in Q\}$, its *multiplication group* $\text{Mlt}(Q)$ and sometimes this group has a strong connection with the structure of Q . This idea of relating loops with groups has been very fruitful for Moufang loops following the work of Glauberman [4] and Doro [2] and especially in recent years [3, 6–8, 12]. Glauberman observed that the multiplication operators on a Moufang loop Q with identity 1 satisfy

$$(1.1) \quad \begin{aligned} P_1 &= L_1 = R_1 = 1, & P_x L_x R_x &= 1, \\ L_{xyx} &= L_x L_y L_x, & R_{xyx} &= R_x R_y R_x, & P_{xyx} &= P_x P_y P_x, \\ L_{y^{-1}x} &= R_y L_x P_y, & R_{y^{-1}x} &= P_y R_x L_y, & P_{y^{-1}x} &= L_y P_x R_y, \\ L_{xy^{-1}} &= P_y L_x R_y, & R_{xy^{-1}} &= L_y R_x P_y & \text{and } P_{xy^{-1}} &= R_y P_x L_y, \end{aligned}$$

2010 *Mathematics Subject Classification.* 16T05, 20N05, 17D99.

Key words and phrases. Triality, Hopf algebras, Moufang-Hopf algebras, Moufang loops, Malcev algebras, Lie algebras, groups, nonassociative algebra.

José M. Pérez-Izquierdo and Sara Madariaga would like to thank Spanish Ministerio de Educación y Ciencia and FEDER MTM 2007-67884-C04-03 and the University of La Rioja. Sara Madariaga also thanks support from Spanish MICINN grant AP2007-01986 and ATUR 09/22.

where $P_x = R_x^{-1}L_x^{-1}$. The group $\mathcal{D}(Q)$ generated by the symbols $\{L_x, R_x, P_x \mid x \in Q\}$ subject to relations (1.1) inherits two automorphisms ρ, σ with $\sigma^2 = \rho^3 = \text{Id}_{\mathcal{D}(Q)}$ and $\sigma\rho = \rho^2\sigma$ such that

$$(1.2) \quad \begin{array}{lll} P_x^\rho = L_x & L_x^\rho = R_x & R_x^\rho = P_x \\ P_x^\sigma = P_x^{-1} & L_x^\sigma = R_x^{-1} & R_x^\sigma = L_x^{-1}, \end{array}$$

due to the symmetries of relations (1.1). They afford a representation of the symmetric group on three letters S_3 as automorphisms of $\mathcal{D}(Q)$. One important insight was that

$$(1.3) \quad (g^{-1}g^\sigma)(g^{-1}g^\sigma)^\rho(g^{-1}g^\sigma)^{\rho^2} = 1$$

holds for any g in $\mathcal{D}(Q)$. Groups G with a representation of S_3 as automorphisms satisfying (1.3) are called *groups with triality* (relative to ρ and σ). Surprisingly enough, Doro showed that the construction of a group with triality from a Moufang loop can be reversed.¹ We present a simple approach by Grishkov and Zavarnitsine to the construction of a Moufang loop from a group with triality instead of Doro's original approach, since the former avoids the use of symmetric spaces and cosets.

Theorem ([7]). *Given a group with triality G , the set $\mathcal{M}(G) = \{g^{-1}g^\sigma \mid g \in G\}$ is a Moufang loop with respect to the multiplication law*

$$m \cdot n = m^{-\rho}nm^{-\rho^2} = n^{-\rho^2}mn^{-\rho} \quad \forall m, n \in \mathcal{M}(G).$$

Any Moufang loop Q is recovered up to isomorphism as $\mathcal{M}(\mathcal{D}(Q))$ [7]. By construction, Doro's group $\mathcal{D}(Q)$ satisfies the following universal property: given G a group with triality such that $\mathcal{M}(G) \cong Q$ then there exists a homomorphism of groups with triality $\mathcal{D}(Q) \rightarrow G$ defined by $P_x \mapsto x, L_x \mapsto x^\rho$ and $R_x \mapsto x^{\rho^2}$ [2, 7].

Mikheev [12] gave another construction of a group with triality $\mathcal{W}(Q)$ with a universal property dual to that of $\mathcal{D}(Q)$: if G is a group with triality such that $\mathcal{M}(G) \cong Q$ and $Z_S(G) = \{1_G\}$ then there exists a monomorphism $G \rightarrow \mathcal{W}(Q)$ of groups with triality, where $Z_S(G)$ denotes the maximal normal subgroup of G where $S = S_3$ acts trivially. Mikheev's paper has no proofs, but they were provided by Grishkov and Zavarnitsine in [7]. The construction of $\mathcal{W}(Q)$ begins with the definition of a *pseudoautomorphism* of a Moufang loop Q ; that is, a pair (A, a) with $A: Q \rightarrow Q$ a bijective map and a an element of Q , the *right companion* of A , related by

$$(xA) \cdot (yA \cdot a) = (x \cdot y)A \cdot a$$

for all $x, y \in Q$. The pseudoautomorphisms of Q form a group $\text{PsAut}(Q)$ with product

$$(A, a)(B, b) = (AB, aB \cdot b).$$

The group $\mathcal{W}(Q)$ is then defined as $\mathcal{W}(Q) = \text{PsAut}(Q) \times Q$ with the product

$$[(A, a), x][(B, b), y] = [(A, a)(B, b)(C, c), xB \cdot y]$$

where

$$(C, c) = (R_{b, xB}, b^{-1}(xB)^{-1}b(xB))(R_{xB, y}, (xB)^{-1}y^{-1}(xB)y)$$

and $R_{x, y} = R_x R_y R_{xy}^{-1}$. The actions of ρ and σ are given by

$$[(A, a), x] \xrightarrow{\rho} [(A, a), a][(T_x, x^{-3}), x^{-2}] \text{ and}$$

¹A detailed and illuminating study of the connections between certain categories of Moufang loops and groups with triality can be found in [10], where a slightly different definition of a group with triality is used.

$$[(A, a), x] \xrightarrow{\sigma} [(A, a)(T_x, x^{-3}), x^{-1}]$$

with $T_x = L_x^{-1}R_x$.

As remarked in [7] a direct verification of the associativity of this product is “technically intractable”. However, this technicality on the definition of $\mathcal{W}(Q)$ is fictitious since this group is just the group of *autotopies* of Q , i.e. triples (A, B, C) of bijective maps from Q to Q such that

$$(xy)A = (xB)(yC)$$

for all $x, y \in Q$, with componentwise product. This group has been known for many years, but its universal property seems to have gone unnoticed until interpreted as $\mathcal{W}(Q)$. This description allows simple proofs of the properties of $\mathcal{W}(Q)$. Section 2 is devoted to this issue. We will also extend these ideas to the context of Hopf algebras in Section 6.

The approach of Grishkov and Zavarnitsine to the construction of $\mathcal{M}(G)$ is well suited for its extension to cocommutative Hopf algebras. Recall Sweedler’s sigma notation $\Delta(u) = \sum u_{(1)} \otimes u_{(2)}$ for the comultiplication in Hopf algebras. The antipode will be usually denoted by S , and ϵ will stand for the counit. Although the antipode and the group generated by ρ and σ are represented by S and \mathbf{S} respectively, this will not lead to confusion. The letter F is reserved for the ground field.

Definition 1.1. Given two automorphisms ρ, σ of a cocommutative Hopf algebra H such that $\sigma^2 = \rho^3 = \text{Id}_H$ and $\sigma\rho = \rho^2\sigma$, H is said to be a cocommutative Hopf algebra with triality relative to ρ and σ in case that

$$(1.4) \quad \sum P(u_{(1)})\rho(P(u_{(2)}))\rho^2(P(u_{(3)})) = \epsilon(u)1,$$

where $P(u) = \sum \sigma(u_{(1)})S(u_{(2)})$.

As we will show, the definition of Hopf algebra with triality does not depend on the generators ρ, σ of the group $\mathbf{S} = \langle \rho, \sigma \rangle$ generated by ρ and σ , so we can talk about Hopf algebras with triality \mathbf{S} , although usually we will explicitly mention some generators ρ and σ . The group algebra FG of a group G with triality relative to ρ and σ is clearly a cocommutative Hopf algebra with triality relative to ρ and σ (we abuse notation by identifying automorphisms of G with their linear extensions to FG) so Hopf algebras with triality are very natural. Since operators are written on the left in this definition, $P(g)$ gives $\sigma(g)g^{-1}$ when applied to a group algebra rather than $P(\sigma(g^{-1})) = g^{-1}\sigma(g)$, which corresponds to the expression $g^{-1}g^\sigma$ appearing in (1.3).

The analog of Moufang loops in the context of Hopf algebras are Moufang-Hopf algebras:

Definition 1.2. Any cocommutative and coassociative unital bialgebra $(U, \Delta, \epsilon, \cdot, 1)$ satisfying the *left Moufang-Hopf identity*

$$(1.5) \quad \sum u_{(1)}(v(u_{(2)}w)) = \sum ((u_{(1)}v)u_{(2)})w$$

will be called a *Moufang-Hopf algebra* in case that there exists a map $S: U \rightarrow U$, the antipode, such that

$$\begin{aligned} \sum S(u_{(1)})(u_{(2)}v) &= \epsilon(u)v = \sum u_{(1)}(S(u_{(2)})v) \text{ and} \\ \sum (vu_{(1)})S(u_{(2)}) &= \epsilon(u)v = \sum (vS(u_{(1)}))u_{(2)}. \end{aligned}$$

Any Moufang-Hopf algebra also satisfies the *middle* and *right Moufang-Hopf identities*:

$$\sum (u_{(1)}(vw))u_{(2)} = \sum (u_{(1)}v)(wu_{(2)}) \text{ and } \sum ((vu_{(1)})w)u_{(2)} = \sum v(u_{(1)}(wu_{(2)})).$$

The *loop algebra* FQ of a Moufang loop Q is an example of Moufang-Hopf algebra (with $\Delta(a) = a \otimes a$, $\epsilon(a) = 1$, and antipode that is the linear extension of $S: a \mapsto a^{-1}$ for any $a \in Q$). Other sources of Moufang-Hopf algebras are the universal enveloping algebras of Malcev algebras. A *Malcev algebra* over a field of characteristic $\neq 2$ is an algebra $(\mathfrak{m}, [\cdot, \cdot])$ with a skew-symmetric product $[x, y]$ that satisfies the Malcev identity

$$J(x, y, [x, z]) = [J(x, y, z), x]$$

where $J(x, y, z) = [[x, y], z] + [[y, z], x] + [[z, x], y]$. In the same way that any associative algebra becomes a Lie algebra with the commutator product, for any nonassociative algebra A the *generalized alternative nucleus*

$$N_{\text{alt}}(A) = \{a \in A \mid (a, x, y) = -(x, a, y) = (x, y, a) \quad \forall x, y \in A\}$$

where $(x, y, z) = (xy)z - x(yz)$, is closed under the commutator $[x, y] = xy - yx$ and with this product becomes a Malcev algebra. Any Lie algebra \mathfrak{g} appears as a (Lie) subalgebra of its universal enveloping algebra $U(\mathfrak{g})$ when the associative product is replaced by the commutator. For Malcev algebras there is a counterpart of this result: any Malcev algebra \mathfrak{m} over a field of characteristic $\neq 2, 3$ appears as a (Malcev) subalgebra of $N_{\text{alt}}(U(\mathfrak{m}))$ for some nonassociative algebra $U(\mathfrak{m})$, namely its universal enveloping algebra [14]. Whenever the Malcev algebra \mathfrak{m} is a Lie algebra, $U(\mathfrak{m})$ is isomorphic to the usual universal enveloping algebra of the Lie algebra \mathfrak{m} . This result was the aim of [14], where it was noticed that $U(\mathfrak{m})$ also has a bialgebra structure. Later, in [13] it was proved that $U(\mathfrak{m})$ is a Moufang-Hopf algebra where \mathfrak{m} embeds as primitive elements, i.e. elements a such that $\Delta(a) = a \otimes 1 + 1 \otimes a$, where Δ stands for the comultiplication. In any Moufang-Hopf algebra, the Moufang-Hopf identities easily imply that primitive elements belong to the generalized alternative nucleus.

The constructions of Glauberger, Doro, Grishkov and Zavaritsine can be extended to cocommutative Hopf algebras with triality in the following terms:

Theorem. *Let H be a cocommutative Hopf algebra with triality relative to ρ and σ and define $P(x) = \sum \sigma(x_{(1)})S(x_{(2)})$ for any $x \in H$. Then*

$$\mathcal{MH}(H) = \{P(x) \mid x \in H\}$$

is a unital cocommutative Moufang-Hopf algebra with the coalgebra structure and antipode inherited from H , the same unit element, and product defined by

$$u * v = \sum \rho^2(S(u_{(1)}))v\rho(S(u_{(2)})) = \sum \rho(S(v_{(1)}))u\rho^2(S(v_{(2)}))$$

for any $u, v \in \mathcal{MH}(H)$.

We will devote Section 3 to proving this result. Doro's construction of $\mathcal{D}(Q)$ can also be extended to the context of Hopf algebras to obtain a converse of this theorem, namely that any cocommutative Moufang-Hopf algebra appears as $\mathcal{MH}(H)$ for a certain Hopf algebra H with triality. In particular, there should be a natural way of constructing the universal enveloping algebra of a Malcev algebra from a Hopf algebra with triality. The development of this approach was the motivation for the present paper.

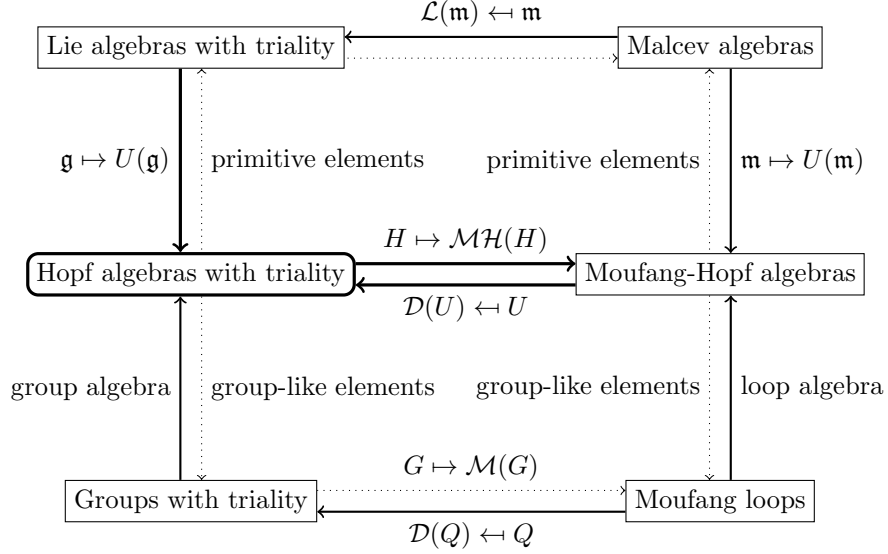


FIGURE 1. Some relations between Moufang/Malcev objects and associative/Lie objects with triality

We need a final ingredient to put all the pieces together, namely, the notion of a Lie algebra with triality that appeared in the work of Mikheev [11] and was studied by Grishkov in [5]. Given a Lie algebra \mathfrak{g} , two automorphisms ρ, σ of \mathfrak{g} such that $\sigma^2 = \rho^3 = \text{Id}_{\mathfrak{g}}$, $\sigma\rho = \rho^2\sigma$ and $\mathbf{S} = \langle \rho, \sigma \rangle$, the group generated by them, \mathfrak{g} is said to be a Lie algebra with triality \mathbf{S} (or relative to ρ and σ) in case that

$$(1.6) \quad a - \sigma(a) + \rho(a) - \rho\sigma(a) + \rho^2(a) - \rho^2\sigma(a) = 0$$

for any $a \in \mathfrak{g}$. The automorphisms ρ, σ induce an action $\lambda: \mathbf{S}_3 \rightarrow \text{Aut}(\mathfrak{g})$ of the symmetric group on three letters \mathbf{S}_3 on \mathfrak{g} by $(12) \mapsto \sigma$, $(123) \mapsto \rho$. Condition (1.6) is equivalent to

$$(1.7) \quad \sum_{\tau \in \mathbf{S}_3} \text{sig}(\tau) \tau(a) = 0,$$

where we write $\tau(a)$ instead of $\lambda(\tau)(a)$ for short. In particular (1.6) does not depend on the choice of the generators ρ, σ of \mathbf{S} .

Section 4 is devoted to proving that the universal enveloping algebra of a Lie algebra with triality is a Hopf algebra with triality, so we can produce Moufang-Hopf algebras from Lie algebras with triality.

In Section 5 we will present a different approach to the construction of the universal enveloping algebra $U(\mathfrak{m})$ of a Malcev algebra \mathfrak{m} in [14]. We start with a Malcev algebra \mathfrak{m} and the Lie algebra $\mathcal{L}(\mathfrak{m})$ defined in [14]. This Lie algebra happens to be a Lie algebra with triality, so its universal enveloping algebra $U(\mathcal{L}(\mathfrak{m}))$ is a Hopf algebra with triality. We will prove that $U(\mathfrak{m})$ is isomorphic to $\mathcal{MH}(U(\mathcal{L}(\mathfrak{m})))$. Figure 1 shows some relations between the objects that we will be concerned with.

2. GROUPS WITH TRIALITY AND MOUFANG LOOPS²

Given a Moufang loop Q , an *autotopy* of Q is a triple (A_1, A_2, A_3) of bijective transformations in $\text{Bij}(Q)$ such that

$$(xy)A_1 = (xA_2)(yA_3)$$

for any $x, y \in Q$. The set $\text{Atp}(Q)$ of all autotopies of Q is a group with the componentwise composition. The Moufang identities imply that

$$(L_x, U_x, L_x^{-1}), (R_x, R_x^{-1}, U_x) \text{ and } (U_x, L_x, R_x)$$

are autotopies of Q , where $U_x = L_x R_x$. There is an action of the symmetric group on three letters as automorphisms of $\text{Atp}(Q)$ given by

$$(2.1) \quad (A_1, A_2, A_3)^\rho = (JA_2J, A_3, JA_1J) \text{ and } (A_1, A_2, A_3)^\sigma = (A_3, JA_2J, A_1)$$

where $J: x \mapsto x^{-1}$ for any $x \in Q$ [17, Proposition 4.1.1]. In addition to the identities that define a Moufang loop, it is convenient to recall that any element x in the loop has an inverse x^{-1} which satisfies $L_x^{-1} = L_{x^{-1}}$ and $R_x^{-1} = R_{x^{-1}}$.

Lemma 2.1. *If $(A_1, A_2, A_3) \in \text{Atp}(Q)$ with $1A_2 = 1$, then $A_1 = A_3$ and $JA_2J = A_2$.*

Proof. The condition on A_2 implies that $(yA_1) = (1y)A_1 = (1A_2)(yA_3) = yA_3$ so $A_1 = A_3$. With $a = 1A_3$ we obtain that $xA_3 = xA_1 = (x1)A_1 = xA_2a$, so $a = 1A_1 = (xx^{-1})A_1 = (xA_2)(x^{-1}A_3) = (xA_2)(x^{-1}A_2a)$. Multiplying by $(xA_2)^{-1}$ we get that $(xA_2)^{-1}a = x^{-1}A_2a$ which gives the result. \square

Compare the following theorem with [7, Corollary 1].

Theorem 2.2. *Let Q be a Moufang loop. Then $\text{Atp}(Q)$ is a group with triality (relative to ρ and σ given by (2.1)) such that $\mathcal{M}(\text{Atp}(Q)) \cong Q$ and $Z_S(\text{Atp}(Q)) = \{1_{\text{Atp}(Q)}\}$. Moreover, $\text{Atp}(Q)$ is a universal injective object in the following sense: if G is any group with triality such that $\mathcal{M}(G) \cong Q$ and $Z_S(G) = \{1_G\}$, then there exists a monomorphism of groups with triality $G \rightarrow \text{Atp}(Q)$.*

Proof. The condition of being a group with triality for $\text{Atp}(Q)$ is equivalent to the following three equalities:

$$\begin{aligned} A_1^{-1}A_3JA_2^{-1}JA_2JA_3^{-1}A_1J &= \text{Id}_Q, \\ A_2^{-1}JA_2JA_3^{-1}A_1JA_1^{-1}A_3J &= \text{Id}_Q \text{ and} \\ A_3^{-1}A_1JA_1^{-1}A_3JA_2^{-1}JA_2J &= \text{Id}_Q. \end{aligned}$$

To check these equalities, we first observe that by choosing $x = 1A_2$, the middle component of $(A_1, A_2, A_3)(R_x, R_x^{-1}, U_x) \in \text{Atp}(Q)$ fixes 1 so, according to Lemma 2.1, $(A_1, A_2, A_3)(R_x, R_x^{-1}, U_x) = (A, B, A)$ for some A, B with $JB = BJ$. Since

$$(A_1, A_2, A_3) = (A, B, A)(R_x^{-1}, R_x, U_x^{-1})$$

²After the first version of this paper was submitted to the editor, Jonathan Hall called our attention to his recent work [9] devoted to proving Theorem 2.4 below for Bol loops, and he provided us with a copy of his preprint [10]. This has led us to remove our proof of Theorem 2.4 from the present version of our paper. Theorem 2.2 has been independently established in [10, Section 10.3]. However, our approach to this result is the motivation for its generalization to Moufang-Hopf algebras in Section 6, and so is included here. We take this opportunity to express our gratitude to Professor Hall for making his work available to us.

and $JL_xJ = R_x^{-1}$ then

$$\begin{aligned} A_1^{-1}A_3JA_2^{-1}JA_2JA_3^{-1}A_1J &= R_xA^{-1}AU_x^{-1}JR_x^{-1}B^{-1}JBR_xJU_xA^{-1}AR_x^{-1}J \\ &= L_x^{-1}JR_x^{-1}JR_xJL_xJ = \text{Id}_Q. \end{aligned}$$

The other identities are proved in a similar way.

The set $\mathcal{M}(\text{Atp}(Q))$ consists of autotopies of the form

$$(2.2) \quad (A_1^{-1}A_3, A_2^{-1}JA_2J, A_3^{-1}A_1).$$

Since in any autotopy (A_1, A_2, A_3) , $(xy)A_1 = (xA_2)(yA_3)$ implies that $A_1 = A_3L_a$ with $a = 1A_2$, then $A_1^{-1}A_3 = L_a^{-1}$ and the autotopy (2.2) can be written as $(L_a^{-1}, A_2^{-1}JA_2J, L_a)$. Again, in any autotopy (A_1, A_2, A_3) the first and second components are related by $A_1 = A_2R_{1A_3}$, so $(L_a^{-1}, A_2^{-1}JA_2J, L_a) = (L_a^{-1}, U_a^{-1}, L_a)$. Since any element a in Q is of the form $1A_2$ for a certain autotopy (A_1, A_2, A_3) , then

$$\mathcal{M}(\text{Atp}(Q)) = \{(L_a^{-1}, U_a^{-1}, L_a) \mid a \in Q\}.$$

The product of $(L_a^{-1}, U_a^{-1}, L_a)$ and $(L_b^{-1}, U_b^{-1}, L_b)$ in $\mathcal{M}(\text{Atp}(Q))$ is

$$\begin{aligned} (L_a^{-1}, U_a^{-1}, L_a) \cdot (L_b^{-1}, U_b^{-1}, L_b) &= (U_a^{-1}, L_a^{-1}, R_a^{-1})(L_b^{-1}, U_b^{-1}, L_b)(R_a, R_a^{-1}, U_a) \\ &= (L_{ab}^{-1}, U_{ab}^{-1}, L_{ab}) \end{aligned}$$

where the last equality follows from the Moufang identities. This proves that $(L_b^{-1}, U_b^{-1}, L_b) \mapsto b$ gives an isomorphism $\mathcal{M}(\text{Atp}(Q)) \cong Q$.

In any group G with triality, $z \in Z_5(G)$ if and only if $z^\tau = z$ and $g^{-1}g^\tau z = zg^{-1}g^\tau$ for any $g \in G$ and $\tau \in \mathbf{S}$, so any $(A_1, A_2, A_3) \in Z_5(\text{Atp}(Q))$ i) satisfies $A_1 = A_2 = A_3$ and ii) commutes with $(L_a^{-1}, U_a^{-1}, L_a)$ for all $a \in Q$. Condition i) implies that A_1 is an automorphism of Q , and condition ii) then says that $A_1 = \text{Id}_Q$. Thus, $Z_5(\text{Atp}(Q)) = \{1_{\text{Atp}(Q)}\}$.

Let G be a group with triality relative to ρ and σ with $\mathcal{M}(G) \cong Q$ (there will be no confusion in using the same letters to denote the automorphisms of G and $\text{Atp}(Q)$). Since

$$x^{-1}(g^{-1}g^\sigma)x^\sigma = (gx)^{-1}(gx)^\sigma \in \mathcal{M}(G)$$

for any $x, g \in G$, we can define maps $A_1, A_2, A_3: G \rightarrow \text{Bij}(\mathcal{M}(G))$ by

$$\begin{aligned} A_1: x &\mapsto A_1(x): m \mapsto x^{-\rho^2\sigma}mx^{\rho^2}, \\ A_2: x &\mapsto A_2(x): m \mapsto x^{-1}mx^\sigma \text{ and} \\ A_3: x &\mapsto A_3(x): m \mapsto x^{-\rho}mx^{\rho\sigma}. \end{aligned}$$

Clearly

$$\begin{aligned} (m \cdot n)^{A_1(x)} &= x^{-\rho^2\sigma}m^{-\rho}nm^{-\rho^2}x^{\rho^2} \\ &= x^{-\sigma\rho}m^{-\rho}x^\rho x^{-\rho}nx^{\rho\sigma}x^{-\sigma\rho^2}m^{-\rho^2}x^{\rho^2} \\ &= (x^{-1}mx^\sigma) \cdot (x^{-\rho}nx^{\rho\sigma}) \\ &= m^{A_2(x)} \cdot n^{A_3(x)} \end{aligned}$$

and $m^{A_1(xy)} = (xy)^{-\rho^2\sigma}m(xy)^{\rho^2} = (m^{A_1(xy)})^{A_1(y)}$ so $A_1(xy) = A_1(x)A_1(y)$. In the same way $A_2(xy) = A_2(x)A_2(y)$ and $A_3(xy) = A_3(x)A_3(y)$. Therefore, we get a homomorphism of groups

$$\begin{aligned} G &\rightarrow \text{Atp}(\mathcal{M}(G)) \\ x &\mapsto (A_1(x), A_2(x), A_3(x)). \end{aligned}$$

One can easily check that this homomorphism is a homomorphism of groups with triality. The kernel of this homomorphism consists of the elements $x \in G$ such that $x^{-1}mx^\sigma = m = x^{-\rho}mx^{\rho\sigma}$ for any $m \in \mathcal{M}(G)$. This is equivalent to $x^\sigma = x = x^\rho$ and $xm = mx$ for all $m \in \mathcal{M}(G)$, so the kernel of the previous homomorphism is $Z_S(G)$. \square

To conclude this section, we would like to describe an explicit isomorphism between $\mathcal{W}(Q)$ and $\text{Atp}(Q)$. First we interpret pseudoautomorphisms in terms of autotopies.

Lemma 2.3. *Let Q be an arbitrary loop. Then the map*

$$\begin{aligned} \{(A_1, A_2, A_3) \in \text{Atp}(Q) \mid 1A_2 = 1\} &\mapsto \text{PsAut}(Q) \\ (A_1, A_2, A_3) &\mapsto (A_2, 1A_1) \end{aligned}$$

is a group isomorphism.

As noted in the proof of Theorem 2.2, any autotopy (A_1, A_2, A_3) of a Moufang loop decomposes in a unique way in $\text{Atp}(Q)$ as

$$(A_1, A_2, A_3) = (A', A, A')(R_x^{-1}, R_x, U_x^{-1})$$

with $x = 1A_2$ and certain A, A' . Hence, we may identify $\text{Atp}(Q)$ with $\text{PsAut}(Q) \times Q$ through $(A_1, A_2, A_3) \mapsto [(A, a), x]$ with $a = 1A'$ and $x = 1A_2$.

Theorem 2.4. *Let Q be a Moufang loop. The map*

$$\begin{aligned} \psi: \text{Atp}(Q) &\rightarrow \mathcal{W}(Q) \\ (A_1, A_2, A_3) &\mapsto [(A, a), x] \end{aligned}$$

with $x = 1A_2$, $A = A_2R_x^{-1}$ and $a = 1A_1x$ is an isomorphism of groups with triality.

The reader may have noticed that in this section most of the operators act on the right of their arguments, which we have done to be consistent with [7]. We will return to this notation in Section 6 where we will consider an analog of autotopies for Moufang-Hopf algebras. In the intervening sections, operators will act on the left of their arguments.

3. COCOMMUTATIVE HOPF ALGEBRAS WITH TRIALITY

In this section we will prove that any cocommutative Hopf algebra H with triality relative to ρ and σ induces a Moufang-Hopf algebra. The arguments are the natural extension of those in [7] to Hopf algebras. We define

$$\mathcal{MH}(H) = \{P(x) \mid x \in H\}$$

where $P(x) = \sum \sigma(x_{(1)})S(x_{(2)})$. Notice that $S(P(x)) = \sigma(P(x)) = P(\sigma(x))$ and that $\Delta(\mathcal{MH}(H)) \subseteq \mathcal{MH}(H) \otimes \mathcal{MH}(H)$.

Lemma 3.1. *For any $u, v \in \mathcal{MH}(H)$ the following hold*

- a) $\sum \rho^i(u_{(1)})\rho^j(u_{(2)}) = \sum \rho^j(u_{(1)})\rho^i(u_{(2)})$ ($i, j \in \{0, 1, 2\}$) and
- b) $\sum \rho^2(S(u_{(1)}))v\rho(S(u_{(2)})) = \sum \rho(S(v_{(1)}))u\rho^2(S(v_{(2)})) \in \mathcal{MH}(H)$.

Proof. On the one hand, condition (1.4) implies that $\sum u_{(1)}\rho(u_{(2)})\rho^2(u_{(3)}) = \epsilon(u)1$ hence $\sum u_{(1)}\rho(u_{(2)}) = S(\rho^2(u))$. On the other hand, equation (1.4) applied to $S(u)$ gives $\sum S(u_{(1)})\rho(S(u_{(2)}))\rho^2(S(u_{(3)})) = \epsilon(u)1$ so $\sum \rho^2(u_{(1)})\rho(u_{(2)})u_{(3)} = \epsilon(u)1$ from

which $\sum \rho(u_{(1)})u_{(2)} = S(\rho^2(u)) = \sum u_{(1)}\rho(u_{(2)})$. This proves part a) in case that $i = 1, j = 0$. The other cases follow from this one by using ρ .

Since $\sigma(u) = S(u)$ and $\sigma(v) = S(v)$, then

$$\begin{aligned} P(\rho(u)\rho(S(v))) &= \sum \sigma(\rho(u_{(1)})\rho(S(v_{(1)})))S(\rho(u_{(2)})\rho(S(v_{(2)}))) \\ &= \sum \rho^2(S(u_{(1)}))\rho^2(v_{(1)})\rho(v_{(2)})S(\rho(u_{(2)})) \\ &= \sum \rho^2(S(u_{(1)}))v\rho(S(u_{(2)})) \end{aligned}$$

and we obtain that $\sum \rho^2(S(u_{(1)}))v\rho(S(u_{(2)})) \in \mathcal{MH}(H)$. In the same way the element $\sum \rho(S(v_{(1)}))u\rho^2(S(v_{(2)}))$ belongs to $\mathcal{MH}(H)$. We can use the triality condition on this element to obtain that

$$\begin{aligned} \epsilon(uv)1 &= \sum \rho(S(v_{(1)}))u_{(1)}\rho^2(S(v_{(2)}))S(v_{(3)})\rho^2(u_{(2)})\rho(S(v_{(4)})) \\ &\quad \rho^2(S(v_{(5)}))\rho(u_{(3)})S(v_{(6)}) \\ &= \sum \rho(S(v_{(1)}))u_{(1)}\rho(v_{(2)})\rho^2(u_{(2)})v_{(3)}\rho(u_{(3)})S(v_{(4)}) \end{aligned}$$

so

$$\begin{aligned} \epsilon(uv)1 &= \sum S(v_{(1)})\rho(S(v_{(2)}))u_{(1)}\rho(v_{(3)})\rho^2(u_{(2)})v_{(4)}\rho(u_{(3)}) \\ &= \sum \rho^2(v_{(1)})u_{(1)}\rho(v_{(2)})\rho^2(u_{(2)})v_{(3)}\rho(u_{(3)}). \end{aligned}$$

This equation implies that $\sum \rho^2(u_{(1)})v\rho(u_{(2)}) = \sum \rho(S(v_{(1)}))S(u)\rho^2(S(v_{(2)}))$. Replacing u by $S(u)$ we get part b). \square

Remark 3.2. Part a) of the lemma shows that the role of ρ and ρ^2 can be switched in the definition of Hopf algebra with triality. Moreover, assume that $\rho\sigma$ is chosen instead of σ and set $Q(x) = \sum \rho\sigma(x_{(1)})S(x_{(2)})$. Then $Q(x) = \rho^2(P(\rho(x)))$ so the triality relation $\sum Q(x_{(1)})\rho(Q(x_{(2)}))\rho^2(Q(x_{(3)})) = \epsilon(x)1$ holds if and only if $\sum P(x_{(1)})\rho(P(x_{(2)}))\rho^2(P(x_{(3)})) = \epsilon(x)1$. Therefore, σ can be replaced by $\rho\sigma$ in the definition of Hopf algebra with triality. The same is true for $\rho^2\sigma$, so the definition does not depend on the generators ρ, σ of the group $S = \langle \rho, \sigma \rangle$.

Theorem 3.3. *Let H be a cocommutative Hopf algebra with triality relative to ρ and σ . Then $\mathcal{MH}(H)$ is a unital cocommutative Moufang-Hopf algebra with the coalgebra structure and antipode inherited from H , the same unit element and product defined by*

$$u * v = \sum \rho^2(S(u_{(1)}))v\rho(S(u_{(2)})) = \sum \rho(S(v_{(1)}))u\rho^2(S(v_{(2)})).$$

Proof. We first observe that since $\Delta(P(x)) = \sum P(x_{(1)}) \otimes P(x_{(2)})$, then $\mathcal{MH}(H)$ is a subcoalgebra of H . The product is well defined because of Lemma 3.1. This product is clearly a homomorphism of coalgebras $\mathcal{MH}(H) \otimes \mathcal{MH}(H) \rightarrow \mathcal{MH}(H)$ so $\mathcal{MH}(H)$ is a (nonassociative) bialgebra. The unit element of H satisfies $1 * v = 1v1 = v$ and $u * 1 = 1u1 = u$ by Lemma 3.1. The antipode S restricts to a

corresponding antipode on $\mathcal{MH}(H)$. In fact,

$$\begin{aligned}
\sum S(u_{(1)}) * (u_{(2)} * v) &= \sum S(u_{(1)}) * (\rho^2(S(u_{(2)}))v\rho(S(u_{(3)}))) \\
&= \sum \rho^2(u_{(1)})\rho^2(S(u_{(2)}))v\rho(S(u_{(3)}))\rho(u_{(4)}) \\
&= \epsilon(u)v \\
&= \sum u_{(1)} * (S(u_{(2)}) * v).
\end{aligned}$$

Since $S(u * v) = \sum \rho(u_{(1)})S(v)\rho^2(u_{(2)}) = S(v) * S(u)$, then we get

$$\sum (v * u_{(1)}) * S(u_{(2)}) = \epsilon(u)v = \sum (v * S(u_{(1)})) * u_{(2)}.$$

Finally,

$$\begin{aligned}
\sum ((u_{(1)} * v) * u_{(2)}) * w &= \sum ((\rho^2(S(u_{(1)}))v\rho(S(u_{(2)}))) * u_{(3)}) * w \\
&= \sum (u_{(1)}\rho^2(S(v_{(1)}))\rho(u_{(2)})u_{(3)}\rho^2(u_{(4)})\rho(S(v_{(2)}))u_{(5)}) * w \\
&= \sum (u_{(1)}\rho^2(S(v_{(1)}))\rho(S(v_{(2)}))u_{(2)}) * w \\
&= \sum (u_{(1)}vu_{(2)}) * w \\
&= \sum \rho^2(S(u_{(1)}))\rho^2(S(v_{(1)}))\rho^2(S(u_{(2)}))w\rho(S(u_{(3)}))\rho(S(v_{(2)}))\rho(S(u_{(4)})) \\
&= \sum u_{(1)} * (\rho^2(S(v_{(1)}))\rho^2(S(u_{(2)}))w\rho(S(u_{(3)}))\rho(S(v_{(2)}))) \\
&= \sum u_{(1)} * (v * (\rho^2(S(u_{(2)}))w\rho(S(u_{(3)}))) \\
&= \sum u_{(1)} * (v * (u_{(2)} * w)).
\end{aligned}$$

□

For any Moufang-Hopf algebra U and $m \in U$ consider $P_m = \sum R_{S(m_{(1)})}L_{S(m_{(2)})}$.

Lemma 3.4. *Let U be a cocommutative Moufang-Hopf algebra. Then for any $m, n \in U$:*

- i) $P_1 = L_1 = R_1 = \text{Id}_U$,
- ii) $\sum P_{m_{(1)}}L_{m_{(2)}}R_{m_{(3)}} = \epsilon(m)\text{Id}_U$,
- iii) $\sum P_{m_{(1)}}P_nP_{m_{(2)}} = \sum P_{m_{(1)}nm_{(2)}}$, $\sum L_{m_{(1)}}L_nL_{m_{(2)}} = \sum L_{m_{(1)}nm_{(2)}}$,
 $\sum R_{m_{(1)}}R_nR_{m_{(2)}} = \sum R_{m_{(1)}nm_{(2)}}$,
- iv) $\sum R_{m_{(1)}}P_nL_{m_{(2)}} = P_{S(m)n}$, $\sum P_{m_{(1)}}L_nR_{m_{(2)}} = L_{S(m)n}$,
 $\sum L_{m_{(1)}}R_nP_{m_{(2)}} = R_{S(m)n}$,
- v) $\sum L_{m_{(1)}}P_nR_{m_{(2)}} = P_{nS(m)}$, $\sum R_{m_{(1)}}L_nP_{m_{(2)}} = L_{nS(m)}$ and
 $\sum P_{m_{(1)}}R_nL_{m_{(2)}} = R_{nS(m)}$.

Proof. Parts i) and ii) are obvious. We will prove the first identities in parts iii), iv) and v). The proofs of the remaining identities are left to the reader.

iii) Using the middle Moufang-Hopf identity,

$$\begin{aligned}
\sum P_{m_{(1)}}P_nP_{m_{(2)}}(x) &= \sum S(m_{(1)})(S(n_{(1)})(S(m_{(2)})xS(m_{(3)}))S(n_{(2)}))S(m_{(4)}) \\
&= \sum S(m_{(1)})(S(n_{(1)})S(m_{(2)}))x(S(n_{(2)})S(m_{(3)}))S(m_{(2)}) \\
&= \sum (S(m_{(1)})S(n_{(1)})S(m_{(2)}))x(S(m_{(3)})S(n_{(2)})S(m_{(4)})) \\
&= \sum P_{m_{(1)}nm_{(2)}}(x).
\end{aligned}$$

iv) The middle and right Moufang-Hopf identities imply

$$\begin{aligned}
\sum R_{m_{(1)}} P_n L_{m_{(2)}}(x) &= \sum (S(n_{(1)})(m_{(2)}x)S(n_{(2)}))m_{(1)} \\
&= \sum (S(n_{(1)})((m_{(1)}xm_{(2)})S(m_{(3)}))S(n_{(2)}))m_{(4)} \\
&= \sum ((S(n_{(1)})(m_{(1)}xm_{(2)}))(S(m_{(3)})S(n_{(2)})))m_{(4)} \\
&= \sum ((S(n_{(1)})(m_{(1)}xm_{(2)}))S(m_{(3)}))(m_{(4)}(S(m_{(5)})S(n_{(2)}))m_{(6)})) \\
&= \sum (S(n_{(1)})m_{(1)})x(S(n_{(2)})m_{(2)}) \\
&= P_{S(m)n}(x).
\end{aligned}$$

v) By the right, middle and left Moufang-Hopf identities

$$\begin{aligned}
\sum L_{m_{(1)}} P_n R_{m_{(2)}}(x) &= \sum m_{(1)}(S(n_{(1)})(xS(m_{(2)}))(m_{(3)}1m_{(4)}))S(n_{(2)}) \\
&= \sum m_{(1)}((S(n_{(1)})(xS(m_{(2)})))((m_{(3)}m_{(4)})S(n_{(2)}))) \\
&= \sum (m_{(1)}(S(n_{(1)})(xS(m_{(2)})))m_{(3)})(S(m_{(4)})((m_{(5)}m_{(6)})S(n_{(2)}))) \\
&= \sum ((m_{(1)}S(n_{(1)}))x)(m_{(2)}S(n_{(2)})) \\
&= P_{nS(m)}(x).
\end{aligned}$$

□

Given a cocommutative Moufang-Hopf algebra U we define $\mathcal{D}(U)$ as the unital associative algebra generated by abstract symbols $\{P_m, L_m, R_m \mid m \in U\}$ subject to the relations

$$\begin{aligned}
P_1 &= L_1 = R_1 = 1, \\
P_{\alpha m + \beta n} &= \alpha P_m + \beta P_n, \quad L_{\alpha m + \beta n} = \alpha L_m + \beta L_n, \quad R_{\alpha m + \beta n} = \alpha R_m + \beta R_n, \\
\sum P_{m_{(1)}} L_{m_{(2)}} R_{m_{(3)}} &= \epsilon(m)1, \\
\sum P_{m_{(1)}} P_n P_{m_{(2)}} &= \sum P_{m_{(1)}nm_{(2)}}, \quad \sum L_{m_{(1)}} L_n L_{m_{(2)}} = \sum L_{m_{(1)}nm_{(2)}}, \\
\sum R_{m_{(1)}} R_n R_{m_{(2)}} &= \sum R_{m_{(1)}nm_{(2)}}, \\
\sum R_{m_{(1)}} P_n L_{m_{(2)}} &= P_{S(m)n}, \quad \sum P_{m_{(1)}} L_n R_{m_{(2)}} = L_{S(m)n}, \\
\sum L_{m_{(1)}} R_n P_{m_{(2)}} &= R_{S(m)n}, \\
\sum L_{m_{(1)}} P_n R_{m_{(2)}} &= P_{nS(m)}, \quad \sum R_{m_{(1)}} L_n P_{m_{(2)}} = L_{nS(m)} \text{ and} \\
\sum P_{m_{(1)}} R_n L_{m_{(2)}} &= R_{nS(m)},
\end{aligned}$$

for any $\alpha, \beta \in F$ and $m, n \in U$. The maps

$$\begin{aligned}
\Delta: P_m &\mapsto \sum P_{m_{(1)}} \otimes P_{m_{(2)}}, \quad L_m \mapsto \sum L_{m_{(1)}} \otimes L_{m_{(2)}}, \quad R_m \mapsto \sum R_{m_{(1)}} \otimes R_{m_{(2)}} \\
\epsilon: P_m &\mapsto \epsilon(m)1, \quad L_m \mapsto \epsilon(m)1, \quad R_m \mapsto \epsilon(m)1 \\
S: P_m &\mapsto P_{S(m)}, \quad L_m \mapsto L_{S(m)}, \quad R_m \mapsto R_{S(m)}
\end{aligned}$$

induce corresponding homomorphisms of algebras $\Delta: \mathcal{D}(U) \rightarrow \mathcal{D}(U) \otimes \mathcal{D}(U)$, $\epsilon: \mathcal{D}(U) \rightarrow F$ and $S: \mathcal{D}(U) \rightarrow \mathcal{D}(U)$ that make $\mathcal{D}(U)$ a cocommutative Hopf

algebra. In fact, $\mathcal{D}(U)$ relative to the automorphisms induced by

$$\begin{array}{ccc} & \rho & \\ P_m & \mapsto & L_m \\ L_m & \mapsto & R_m \\ R_m & \mapsto & P_m \end{array} \quad \begin{array}{ccc} & \sigma & \\ P_m & \mapsto & P_{S(m)} \\ L_m & \mapsto & R_{S(m)} \\ R_m & \mapsto & L_{S(m)} \end{array}$$

is a Hopf algebra with triality.

Theorem 3.5. *For any cocommutative Moufang-Hopf algebra U , the map*

$$\begin{array}{ccc} \iota: U & \rightarrow & \mathcal{MH}(\mathcal{D}(U)) \\ m & \mapsto & P_m \end{array}$$

is an isomorphism of Moufang-Hopf algebras. Moreover, $\mathcal{D}(U)$ satisfies the following universal property: given a Hopf algebra with triality H and a homomorphism $\varphi: U \rightarrow \mathcal{MH}(H)$ of Moufang-Hopf algebras, φ extends to a homomorphism $\bar{\varphi}: \mathcal{D}(U) \rightarrow H$ of Hopf algebras with triality (i.e. commutes with the action of ρ and σ) such that the diagram

$$\begin{array}{ccc} & \mathcal{D}(U) & \\ & \nearrow \iota & \downarrow \bar{\varphi} \\ U & \xrightarrow{\varphi} & H \end{array}$$

commutes.

Proof. Let us first prove that ι is an isomorphism of Moufang-Hopf algebras. If $P_m = P_n$ then $L_m = \rho(P_m) = \rho(P_n) = L_n$. However, Lemma 3.4 implies that there exists a homomorphism from $\mathcal{D}(U)$ to the multiplication algebra of U that sends L_m to the left multiplication operator by m . Evaluating on 1, we obtain that $m = n$. Thus, ι is injective. In order to check that ι is a homomorphism of algebras observe that

$$\begin{aligned} \iota(m) * \iota(n) &= P_m * P_n = \sum \rho^2(S(P_{m(1)}))P_n\rho(S(P_{m(2)})) \\ &= \sum R_{S(m(1))}P_nL_{S(m(2))} = P_{mn} \\ &= \iota(mn). \end{aligned}$$

By the definition of Δ , ϵ and S it is easily seen that ι is a homomorphism of Moufang-Hopf algebras. To prove that the map ι is surjective, we must check that $\mathcal{MH}(\mathcal{D}(U)) = \{P_m \mid m \in U\}$. By definition, $\mathcal{MH}(\mathcal{D}(U)) = \{P(x) \mid x \in \mathcal{D}(U)\}$ but $P(xy) = \sum \sigma(x_{(1)})P(y)S(x_{(2)})$, so we only need to prove that

$$P(P_m), P(L_m), P(R_m) \in \mathcal{MH}(\mathcal{D}(U))$$

and that for any $m, n \in U$,

$$\sum \sigma(P_{n(1)})P_mS(P_{n(2)}), \sum \sigma(L_{n(1)})P_mS(L_{n(2)}), \sum \sigma(R_{n(1)})P_mS(R_{n(2)})$$

also belong to $\mathcal{MH}(\mathcal{D}(U))$. By the definition and relations on $\mathcal{D}(U)$

$$\begin{aligned} P(P_m) &= \sum \sigma(P_{m(1)})S(P_{m(2)}) = \sum P_{S(m(1))}P_{S(m(2))} = \sum P_{S(m(1))S(m(2))}, \\ P(L_m) &= \sum \sigma(L_{m(1)})S(L_{m(2)}) = \sum R_{S(m(1))}L_{S(m(2))} = P_m \text{ and} \\ P(R_m) &= \sum \sigma(R_{m(1)})S(R_{m(2)}) = \sum L_{S(m(1))}R_{S(m(2))} = P_m \end{aligned}$$

so $P(P_m), P(L_m)$ and $P(R_m)$ belong to $\mathcal{MH}(\mathcal{D}(U))$. The relations on $\mathcal{D}(U)$ also imply that

$$\begin{aligned} \sum \sigma(P_{n_{(1)}})P_m S(P_{n_{(2)}}) &= \sum P_{S(n_{(1)})}P_m P_{S(n_{(2)})} = P_{\sum S(n_{(1)})m S(n_{(2)})}, \\ \sum \sigma(L_{n_{(1)}})P_m S(L_{n_{(2)}}) &= \sum R_{S(n_{(1)})}P_m L_{S(n_{(2)})} = P_{nm} \text{ and} \\ \sum \sigma(R_{n_{(1)}})P_m S(R_{n_{(2)}}) &= \sum L_{S(n_{(1)})}P_m R_{S(n_{(2)})} = P_{mn} \end{aligned}$$

so ι is surjective.

Let $\varphi: U \rightarrow \mathcal{MH}(H)$ be a homomorphism of Moufang-Hopf algebras where H is a cocommutative Hopf algebra with triality. Given $m, n \in U$, the elements $\varphi(m), \varphi(n)$ satisfy

$$\sum \varphi(m_{(1)})\rho(\varphi(m_{(2)}))\rho^2(\varphi(m_{(3)})) = \epsilon(m),$$

and by the definition of the product $*$ of $\mathcal{MH}(H)$,

$$\begin{aligned} \sum \varphi(m_{(1)})\varphi(n)\varphi(m_{(2)}) &= \sum m_{(1)} * n * m_{(2)}, \\ \sum \rho^2(\varphi(m_{(1)}))\varphi(n)\rho(\varphi(m_{(2)})) &= \varphi(S(m)) * \varphi(n) \text{ and} \\ \sum \rho(\varphi(m_{(1)}))\varphi(n)\varphi^2(m_{(2)}) &= \varphi(n) * \varphi(S(m)). \end{aligned}$$

These identities and the others obtained under the action of ρ show that the correspondence

$$\bar{\varphi}: P_m \mapsto \varphi(m), \quad L_m \mapsto \rho(\varphi(m)), \quad R_m \mapsto \rho^2(\varphi(m))$$

induces a homomorphism $\bar{\varphi}: \mathcal{D}(U) \rightarrow H$ of Hopf algebras with triality that makes the diagram in the statement commutative. \square

4. LIE ALGEBRAS WITH TRIALITY

Before any further considerations, let us present the standard example of a Lie algebra with triality. Let $\mathbb{O} = \mathbb{O}(\alpha, \beta, \gamma)$ be a generalized Cayley algebra with norm $n(\cdot)$ over a field of characteristic $\neq 2, 3$; \mathbb{O}_0 the Malcev algebra of traceless elements in \mathbb{O} ; and $\mathfrak{o}(\mathbb{O}, n)$ the orthogonal Lie algebra of all $d \in \text{End}(\mathbb{O})$ which are skewsymmetric relative to $n(\cdot)$ [18]. The (local) Principle of Triality [16] ensures that for any $d_1 \in \mathfrak{o}(\mathbb{O}, n)$ there exist unique $d_2, d_3 \in \mathfrak{o}(\mathbb{O}, n)$ such that

$$(4.1) \quad d_1(xy) = d_2(x)y + xd_3(y)$$

for any $x, y \in \mathbb{O}$. The maps $d_1 \mapsto d_2$ and $d_1 \mapsto d_3$ are automorphisms of $\mathfrak{o}(\mathbb{O}, n)$. An explicit description is known. Recall that $\mathfrak{o}(\mathbb{O}, n) = \text{Der}(\mathbb{O}) \oplus \langle L_a \mid a \in \mathbb{O}_0 \rangle \oplus \langle R_b \mid b \in \mathbb{O}_0 \rangle$ and that the alternative laws $x(xy) = x^2y$, $(yx)x = yx^2$ are equivalent to the following relations

$$L_a(xy) = T_a(x)y - xL_a(y) \quad \text{and} \quad R_a(xy) = -R_a(x)y + xT_a(y)$$

where L_a, R_a denote the left and right multiplication operators by a , and $T_a = L_a + R_a$. Hence the automorphisms $d_1 \mapsto d_2$ and $d_1 \mapsto d_3$ are determined by

$$\begin{array}{ccc} d & \mapsto & d \\ L_a & \mapsto & T_a \\ R_a & \mapsto & -R_a \end{array} \quad \text{and} \quad \begin{array}{ccc} d & \mapsto & d \\ L_a & \mapsto & -L_a \\ R_a & \mapsto & T_a \end{array}$$

for any $d \in \text{Der}(\mathbb{O})$ and $a \in \mathbb{O}_0$. This proves that the maps $\rho, \sigma: \mathfrak{o}(\mathbb{O}, n) \rightarrow \mathfrak{o}(\mathbb{O}, n)$ given by

$$\begin{array}{ccc} d & \xrightarrow{\rho} & d \\ L_a & \mapsto & R_a \\ R_a & \mapsto & -T_a \end{array} \quad \text{and} \quad \begin{array}{ccc} d & \xrightarrow{\sigma} & d \\ L_a & \mapsto & -R_a \\ R_a & \mapsto & -L_a \end{array}$$

are automorphisms, and $\mathfrak{o}(\mathbb{O}, n)$ is a Lie algebra with triality relative to ρ and σ .

In this section we will prove that the universal enveloping algebra of a Lie algebra with triality is a Hopf algebra with triality. In the following, $E(\xi; f)$ will denote the eigenspace of f corresponding to the eigenvalue ξ . After extending scalars if necessary, we may assume that our base field F contains a primitive cube root of unity ω .

Lemma 4.1. *Let \mathfrak{g} be a Lie algebra, $\lambda: S_3 \rightarrow \text{Aut}(\mathfrak{g})$ an action of S_3 as automorphisms of \mathfrak{g} and $\sigma = \lambda((12))$. Then*

$$\{P(x) \mid x \in U(\mathfrak{g})\} = \text{span}\langle a_n \circ (\cdots (a_2 \circ a_1)) \mid a_1, \dots, a_n \in E(-1; \sigma), n \in \mathbb{N} \rangle$$

where $P(x) = \sum \sigma(x_{(1)})S(x_{(2)})$ and $a \circ x = ax + xa$.

Proof. We proceed by induction on the filtration degree of $x \in U(\mathfrak{g})$. In case that $x = a \in \mathfrak{g}$, $P(a) = \sigma(a) - a \in E(-1; \sigma)$. In general, given $a_1 \cdots a_{n+1} \in U(\mathfrak{g})$, we may assume that $a_i \in E(-1; \sigma) \cup E(1; \sigma)$, $i = 1, \dots, n+1$. We distinguish two cases:

- i) *At least one a_i belongs to $E(1; \sigma)$:* in this case, up to terms of lower degree we may assume that $a_{n+1} \in E(1; \sigma)$. With $x = a_1 \cdots a_n$, $a = a_{n+1}$ we obtain

$$P(xa) = \sum \sigma(x_{(1)})\sigma(a)S(x_{(2)}) - \sum \sigma(x_{(1)})aS(x_{(2)}) = 0$$

- ii) $a_1, \dots, a_{n+1} \in E(-1; \sigma)$: In this case, with $x = a_2 \cdots a_{n+1}$ and $a = a_1$ we have

$$P(ax) = \sum \sigma(a)\sigma(x_{(1)})S(x_{(2)}) - \sum \sigma(x_{(1)})S(x_{(2)})a = -a \circ P(x)$$

and the result follows by induction. □

Lemma 4.2. *Given a Lie algebra \mathfrak{g} over a field of characteristic $\neq 2, 3$ and two automorphisms σ, ρ with $\sigma^2 = \rho^3 = \text{Id}_{\mathfrak{g}}$ and $\sigma\rho = \rho^2\sigma$, then \mathfrak{g} is a Lie algebra with triality relative to ρ and σ if and only if $E(1; \rho) \subseteq E(1; \sigma)$.*

Proof. Given $a \in E(1; \rho)$, (1.6) implies that $3\sigma(a) - 3a = 0$ so $\sigma(a) = a$. Conversely, for elements $a \in E(1; \rho)$ condition (1.6) follows from our hypothesis, while for elements $a \in E(\omega; \rho)$, we have that $\sum_{\tau \in S_3} \text{sig}(\tau)\tau(a) = (1 + \omega + \omega^2)(a - \sigma(a)) = 0$. Since $\mathfrak{g} = E(1; \rho) \oplus E(\omega; \rho) \oplus E(\omega^2; \rho)$ we are done. □

The universal enveloping algebra $U(\mathfrak{g})$ of a Lie algebra \mathfrak{g} acts on \mathfrak{g} by

$$x \cdot a = \sum x_{(1)}aS(x_{(2)})$$

where S denotes the antipode. With this notation we have:

Lemma 4.3. *Let \mathfrak{g} be a Lie algebra with triality relative to ρ and σ over a field of characteristic $\neq 2, 3$. Then $U(\mathfrak{g})$ satisfies*

$$(4.2) \quad \begin{aligned} &\epsilon(x)a - P(x) \cdot \sigma(a) + P(x) \cdot \rho(a) \\ &\quad - \rho^2 \sigma(P(x)) \cdot \rho \sigma(a) + \rho^2 \sigma(P(x)) \cdot \rho^2(a) - \epsilon(x) \rho^2(\sigma(a)) = 0. \end{aligned}$$

Proof. First observe that $\sigma\rho = \rho^2\sigma$ implies that

$$\sigma(E(\omega; \rho)) = E(\omega^2; \rho).$$

In particular, by Lemma 4.2 any element $a \in E(-1; \sigma)$ can be written as $a = a' - a''$ with $a' \in E(\omega; \rho)$ and $a'' = \sigma(a')$. Also observe that by Lemma 4.1 we may assume that $P(x) = a_n \circ (\cdots (a_2 \circ a_1))$ with $a_1, \dots, a_n \in E(-1; \sigma)$. This implies that $\sigma(P(x)) = (-1)^n P(x)$.

By Lemma 4.2 the result is obvious if $a \in E(1; \rho)$, so we may assume that $a \in E(\omega; \rho) \cup E(\omega^2; \rho)$. In fact, we only have to prove (4.2) for $a = a' \in E(\omega; \rho)$ because the case $a \in E(\omega^2; \rho)$ is a consequence of the former by applying σ to (4.2).

Let us denote $p = a_n \circ (\cdots (a_2 \circ a_1))$. If $n = 0$ then $p = 1$ and (4.2) is (1.6), so we may assume that $n \geq 1$. Equation (4.2) can be written as

$$(4.3) \quad -p \cdot a'' + \omega p \cdot a' - (-1)^n \omega^2 \rho^2(p) \cdot a'' + (-1)^n \omega^2 \rho^2(p) \cdot a' = 0$$

with $a'' = \sigma(a')$.

To simplify computations we will write p_0, p', p'' for the projections of p on $E(1; \rho), E(\omega; \rho), E(\omega^2; \rho)$ where ρ also denotes the extension of ρ to an automorphism of $U(\mathfrak{g})$. Observe that $\sigma(p) = (-1)^n p$ implies that $\sigma(p_0) = (-1)^n p_0$, $\sigma(p') = (-1)^n p''$ and $\sigma(p'') = (-1)^n p'$.

Plugging $p = p_0 + p' + p''$ into (4.3) and taking projections onto $E(1; \rho), E(\omega; \rho)$ and $E(\omega^2; \rho)$ we get that (4.3) is equivalent to

- (i) $-\omega p' \cdot a'' + \omega^2 p'' \cdot a' = -(-1)^n (-\omega^2 p' \cdot a'' + \omega p'' \cdot a'),$
- (ii) $p_0 \cdot a' - \omega^2 p'' \cdot a'' = -(-1)^n (\omega p_0 \cdot a' - \omega^2 p'' \cdot a'')$ and
- (iii) $\omega p' \cdot a' - p_0 \cdot a'' = -(-1)^n (\omega p' \cdot a' - \omega^2 p_0 \cdot a'').$

Therefore, we need to prove (i), (ii) and (iii).

In order to prove (i) we notice that $-\omega p' \cdot a'' + \omega^2 p'' \cdot a' \in E(1; \rho) \cap \mathfrak{g}$. By Lemma 4.2 we get $-\omega p' \cdot a'' + \omega^2 p'' \cdot a' = \sigma(-\omega p' \cdot a'' + \omega^2 p'' \cdot a') = -(-1)^n \omega p'' \cdot a' + (-1)^n \omega^2 p' \cdot a''$, as desired.

Equality (iii) follows from (ii) by applying σ to it.

We split the proof of (ii) into two cases depending on the parity of n . If n is odd then (ii) is equivalent to

$$(odd) \quad p_0 \cdot a' = 0,$$

while in case that n is even, (ii) is equivalent to

$$(even) \quad p_0 \cdot a' = -2p'' \cdot a''$$

We will use induction on n . Let us assume that (4.3) holds for p and consider $q = b \circ p$ with $b = b' - b'' \in E(-1; \sigma)$, $b' \in E(\omega; \rho)$ and $b'' = \sigma(b')$. The projections of q on $E(1; \rho), E(\omega; \rho)$ and $E(\omega^2; \rho)$ are

$$\begin{aligned} q_0 &= b'p'' + p''b' - b''p' - p'b'', \\ q' &= b'p_0 + p_0b' - b''p'' - p''b'' \text{ and} \\ q'' &= -p_0b'' - b''p_0 + b'p' + p'b' \end{aligned}$$

respectively.

Let us assume that n is odd. In this case we should prove that $q_0 \cdot a' = -2q'' \cdot a''$. First observe that the hypothesis of induction implies that $p_0 \cdot a' = 0$. Applying σ to both sides of this equality we also obtain that $p_0 \cdot a'' = 0$. Equality (i) implies that $p' \cdot a'' = -p'' \cdot a'$. The commutator $[b'', a']$ belongs to $E(1; \rho)$ so, by Lemma 4.2, $[b'', a'] = [b', a'']$. With this information we compute $q_0 \cdot a' + 2q'' \cdot a''$ as follows

$$\begin{aligned} q_0 \cdot a' + 2q'' \cdot a'' &= (b'p'' + p''b' - b''p' - p'b'') \cdot a' + 2(b'p' + p'b') \cdot a'' \\ &= (p''b' - b''p') \cdot a' + (b'p' + p'b') \cdot a'' \\ &= (p''b' - b''p') \cdot a' + (-b'p'' + p'b'') \cdot a' \\ &= -([b', p''] + [b'', p']) \cdot a'. \end{aligned}$$

Since $[b' + b'', a_i] \in E(-1; \sigma)$ and $[b' + b'', p] = \sum_{i=1}^n a_n \circ (\cdots ([b' + b'', a_i] \circ (\cdots (a_2 \circ a_1))))$ by (even) the action of the projection of $[b' + b'', p]$ on $E(1; \rho)$ kills a' . This projection is clearly $[b', p''] + [b'', p']$ so $([b', p''] + [b'', p']) \cdot a' = 0$. This proves that $q_0 \cdot a' = -2q'' \cdot a''$.

Let us assume now that n is even. In this case we should prove that $q_0 \cdot a' = 0$. The hypothesis of induction and (i), (ii) and (iii) for p imply that $p' \cdot a'' = p'' \cdot a'$, $p_0 \cdot a' = -2p'' \cdot a''$ and $p_0 \cdot a'' = -2p' \cdot a'$. The hypothesis of induction applied to $[b' + b'', p] = ([b', p''] + [b'', p']) + ([b', p_0] + [b'', p'']) + ([b'', p_0] + [b', p'])$ also implies that $([b', p''] + [b'', p']) \cdot a' = -2([b', p'] + [b'', p_0]) \cdot a''$. Hence

$$\begin{aligned} 0 &= ([b', p''] + [b'', p']) \cdot a' + 2([b', p'] + [b'', p_0]) \cdot a'' \\ &= 3b'p'' \cdot a' - p''b' \cdot a' + b''p' \cdot a' - p'b'' \cdot a' - 2p'b' \cdot a'' - 4b''p' \cdot a' + 4p''b' \cdot a' \\ &= 3b'p'' \cdot a' + 3p''b' \cdot a' - 3b''p' \cdot a' - 3p'b'' \cdot a' \\ &= 3q_0 \cdot a'. \end{aligned}$$

Since the characteristic of the base field is $\neq 2, 3$ then $q_0 \cdot a' = 0$. This concludes the proof. \square

Theorem 4.4. *Let \mathfrak{g} be a Lie algebra with triality relative to ρ and σ over a field of characteristic $\neq 2, 3$. Then $U(\mathfrak{g})$ is a Hopf algebra with triality relative to ρ and σ .*

Proof. We will prove (1.4) by induction on the filtration degree of $x \in U(\mathfrak{g})$. If this degree is 0 then (1.4) holds trivially. So, let us assume that (1.4) holds for $x \in U(\mathfrak{g})$ of filtration degree $\leq n$ and let us prove that it also is valid for ax with $a \in \mathfrak{g}$. Recall that $P(ax) = \sigma(a)P(x) - P(x)a$.

Since by induction we have that $\sum P(x_{(1)})\rho(P(x_{(2)}))\rho^2(P(x_{(3)})) = \epsilon(x)1$ then $\sum \rho(P(x_{(1)}))\rho^2(P(x_{(2)})) = S(P(x))$ and $\sum P(x_{(1)})\rho(P(x_{(2)})) = S(\rho^2(x))$. Hence

$$\begin{aligned} &\sum P((ax)_{(1)})\rho(P((ax)_{(2)}))\rho^2(P((ax)_{(3)})) \\ &= \sum P(ax_{(1)})\rho(P(x_{(2)}))\rho^2(P(x_{(3)})) + P(x_{(1)})\rho(P(ax_{(2)}))\rho^2(P(x_{(3)})) \\ &\quad + \sum P(x_{(1)})\rho(P(x_{(2)}))\rho^2(P(ax_{(3)})) \\ &= \sum (\sigma(a)P(x_{(1)}) - P(x_{(1)})a) S(P(x_{(2)})) \\ &\quad + P(x_{(1)})\rho(\sigma(a)P(x_{(2)}) - P(x_{(2)})a)\rho^2(P(x_{(3)})) \\ &\quad + \sum S(\rho^2(P(x_{(1)})))\rho^2(\sigma(a)P(x_{(2)}) - P(x_{(2)})a) \end{aligned}$$

$$\begin{aligned}
&= \epsilon(x)\sigma(a) - \sum P(x_{(1)})aS(P(x_{(2)})) \\
&\quad + \sum P(x_{(1)})\rho\sigma(a)S(P(x_{(2)})) - \sum S(\rho^2(P(x_{(1)})))\rho(a)\rho^2(P(x_{(2)})) \\
&\quad + \sum S(\rho^2(P(x_{(1)})))\rho^2\sigma(a)\rho^2(P(x_{(2)})) - \epsilon(x)\rho^2(a) \\
&= \epsilon(x)\sigma(a) - P(x) \cdot a + P(x) \cdot \rho\sigma(a) - \rho^2\sigma(P(x)) \cdot \rho(a) \\
&\quad + \rho^2\sigma(P(x)) \cdot \rho^2\sigma(a) - \epsilon(x)\rho^2(a).
\end{aligned}$$

Lemma 4.3 applied to $\sigma(a)$ then implies

$$\sum P((xa)_{(1)})\rho(P((xa)_{(2)}))\rho^2(P((xa)_{(3)})) = 0 = \epsilon(xa)1.$$

□

5. THE UNIVERSAL ENVELOPING ALGEBRA OF A MALCEV ALGEBRA

In [14], the construction of the universal enveloping algebra of a Malcev algebra \mathfrak{m} over a field F of characteristic $\neq 2, 3$ begins by attaching a Lie algebra $\mathcal{L}(\mathfrak{m})$ to the Malcev algebra \mathfrak{m} . This Lie algebra is the Lie algebra generated by the symbols $\{\lambda_a, \rho_a \mid a \in \mathfrak{m}\}$ subject to the relations

$$\begin{aligned}
(5.1) \quad &\lambda_{\alpha a + \beta b} = \alpha\lambda_a + \beta\lambda_b & \rho_{\alpha a + \beta b} &= \alpha\rho_a + \beta\rho_b \\
&[\lambda_a, \lambda_b] = \lambda_{[a,b]} - 2[\lambda_a, \rho_b] & [\rho_a, \rho_b] &= -\rho_{[a,b]} - 2[\lambda_a, \rho_b] \\
&[\lambda_a, \rho_b] = [\rho_a, \lambda_b]
\end{aligned}$$

for any $a, b \in \mathfrak{m}$, $\alpha, \beta \in F$. With the notation

$$\text{ad}_a = \lambda_a - \rho_a, \quad T_a = \lambda_a + \rho_a \quad \text{and} \quad D_{a,b} = \text{ad}_{[a,b]} - 3[\lambda_a, \rho_b]$$

it was proved that $\mathcal{L}(\mathfrak{m}) = \mathcal{L}_+ \oplus \mathcal{L}_-$ with $\mathcal{L}_+ = \text{span}\langle \text{ad}_a, D_{a,b} \mid a, b \in \mathfrak{m} \rangle$ and $\mathcal{L}_- = \text{span}\langle T_a \mid a \in \mathfrak{m} \rangle$; the mapping $T_a \mapsto a$ being a linear isomorphism from \mathcal{L}_- onto \mathfrak{m} [14, Proposition 3.2]. The underlying vector space of $U(\mathfrak{m})$ was the symmetric algebra $\mathcal{S}(\mathcal{L}_-)$ on \mathcal{L}_- , where a structure of an $\mathcal{L}(\mathfrak{m})$ -module was given. It also was observed that $\mathcal{L}(\mathfrak{m})$ admits two automorphisms ζ, η determined by

$$\begin{aligned}
\zeta(\lambda_a) &= T_a & \eta(\lambda_a) &= -\lambda_a \\
\zeta(\rho_a) &= -\rho_a & \eta(\rho_a) &= T_a
\end{aligned}$$

With these automorphisms, the structure of the $\mathcal{L}(\mathfrak{m})$ -module of $\mathcal{S}(\mathfrak{m})$ (\mathcal{L}_- is identified with \mathfrak{m}) is twisted to get two new modules $\mathcal{S}(\mathfrak{m})_\zeta, \mathcal{S}(\mathfrak{m})_\eta$. The product of $U(\mathfrak{m})$ is obtained as a homomorphism of $\mathcal{L}(\mathfrak{m})$ -modules $\mathcal{S}(\mathfrak{m})_\zeta \otimes \mathcal{S}(\mathfrak{m})_\eta \rightarrow \mathcal{S}(\mathfrak{m})$ satisfying certain conditions [14, Proposition 3.4].

Proposition 5.1. *Let \mathfrak{m} be a Malcev algebra over a field of characteristic $\neq 2, 3$. Then $\mathcal{L}(\mathfrak{m})$ is a Lie algebra with triality relative to $\rho = \eta\zeta$ and $\sigma = \zeta\eta\zeta$.*

Proof. The automorphisms ρ, σ are determined by their action on the generators

$$\begin{aligned}
\sigma(\lambda_a) &= -\rho_a & \rho(\lambda_a) &= \rho_a \\
\sigma(\rho_a) &= -\lambda_a & \rho(\rho_a) &= -T_a
\end{aligned}$$

Thus they clearly satisfy $\sigma^2 = \text{Id}_{\mathcal{L}(\mathfrak{m})} = \rho^3$ and $\sigma\rho = \rho^2\sigma$. Because of (5.1), the elements $\text{ad}_a, D_{a,b}$ are fixed by σ so it suffices to check (1.6) for elements T_a , but this is obvious. □

By Theorem 4.4, the universal enveloping algebra $U(\mathcal{L}(\mathfrak{m}))$ of $\mathcal{L}(\mathfrak{m})$ is then a Hopf algebra with triality, so we can consider the Moufang-Hopf algebra $\mathcal{MH}(U(\mathcal{L}(\mathfrak{m})))$.

Lemma 5.2. *For any $a \in \mathfrak{m}$ and $u \in \mathcal{MH}(U(\mathcal{L}(\mathfrak{m})))$ the elements $T_a * u + u * T_a \in \mathcal{MH}(U(\mathcal{L}(\mathfrak{m})))$ and $T_a u + u T_a \in U(\mathcal{L}(\mathfrak{m}))$ coincide.*

Proof. We use both formulas for the product on $\mathcal{MH}(\mathcal{L}(\mathfrak{m}))$ in Theorem 3.3. On the one hand $T_a * u = \rho^2(S(T_a))u + u\rho(S(T_a)) = \rho_a u + u\lambda_a$. On the other hand, $u * T_a = \rho(S(T_a))u + u\rho^2(S(T_a)) = \lambda_a u + u\rho_a$. Thus $T_a * u + u * T_a = T_a u + u T_a$. \square

Theorem 5.3. *Let \mathfrak{m} be a Malcev algebra over a field of characteristic $\neq 2, 3$. Then $U(\mathfrak{m})$ is isomorphic to $\mathcal{MH}(U(\mathcal{L}(\mathfrak{m})))$.*

Proof. Lemma 4.1 and Lemma 5.2 imply that $\mathcal{MH}(U(\mathcal{L}(\mathfrak{m})))$ is spanned by elements of the form $T_{a_n} \bullet (\cdots (T_{a_2} \bullet T_{a_1}))$ with $a_1, \dots, a_n \in \mathfrak{m}$, $n \in \mathbb{N}$ and $T_a \bullet u = T_a * u + u * T_a$. The elements T_a are primitive inside the Moufang-Hopf algebra $\mathcal{MH}(U(\mathcal{L}(\mathfrak{m})))$, so they belong to the generalized alternative nucleus. The commutator of two of them in $\mathcal{MH}(U(\mathcal{L}(\mathfrak{m})))$ is easily computed:

$$\begin{aligned} T_a * T_b &= \rho^2(S(T_a))T_b + T_b\rho(S(T_a)) = \rho_a T_b + T_b \lambda_a, \\ T_a * T_b - T_b * T_a &= \rho_a \rho_b + \lambda_b \lambda_a - \rho_b \rho_a - \lambda_a \lambda_b = [\rho_a, \rho_b] - [\lambda_a, \lambda_b] = -T_{[a, b]} \end{aligned}$$

where the last equality follows from relations (5.1). By the universal property of $U(\mathfrak{m})$ in [14], we can conclude that the map $a \mapsto -T_a$ extends to a homomorphism of unital algebras $\varphi: U(\mathfrak{m}) \rightarrow \mathcal{MH}(U(\mathcal{L}(\mathfrak{m})))$. In fact, since $\mathcal{MH}(U(\mathcal{L}(\mathfrak{m}))) = \text{span}\langle T_{a_n} \bullet (\cdots (T_{a_2} \bullet T_{a_1})) \mid a_1, \dots, a_n \in \mathfrak{m}, n \in \mathbb{N} \rangle$, then φ is surjective. To prove that φ is an isomorphism we appeal to the Poincaré-Birkhoff-Witt Theorem for $U(\mathfrak{m})$ and $U(\mathcal{L}(\mathfrak{m}))$. Given a totally ordered basis $\{a_i\}_{i \in \Lambda}$ of \mathfrak{m} , $U(\mathfrak{m})$ admits a basis $\{a_{i_n} \bullet (\cdots (a_{i_2} \bullet a_{i_1})) \mid i_1 \leq \cdots \leq i_n, n \in \mathbb{N}\}$ with $a \bullet x = ax + xa$ in $U(\mathfrak{m})$ [14]. This basis is sent to $\{T_{a_{i_n}} \circ (\cdots (T_{a_{i_2}} \circ T_{a_{i_1}})) \mid i_1 \leq \cdots \leq i_n, n \in \mathbb{N}\}$, a linearly independent set in $U(\mathcal{L}(\mathfrak{m}))$. Since φ sends a basis to a linearly independent set, then φ is also injective. \square

Theorem 5.4. *Let \mathfrak{m} be a Malcev algebra over a field of characteristic $\neq 2, 3$. Then $\mathcal{D}(U(\mathfrak{m}))$ is isomorphic to $U(\mathcal{L}(\mathfrak{m}))$.*

Proof. The isomorphism $\varphi: U(\mathfrak{m}) \rightarrow \mathcal{MH}(U(\mathcal{L}(\mathfrak{m})))$ in the proof of Theorem 5.3 sends $a \in \mathfrak{m}$ to $-T_a$. By the universal property of $\mathcal{D}(U(\mathfrak{m}))$ we obtain a homomorphism $\bar{\varphi}: \mathcal{D}(U(\mathfrak{m})) \rightarrow U(\mathcal{L}(\mathfrak{m}))$ of Hopf algebras with triality that sends P_a to $-T_a$. The relations that define $\mathcal{D}(U(\mathfrak{m}))$ imply that most of the generators $\{P_m, L_m, R_m \mid m \in U(\mathfrak{m})\}$ are superfluous. In fact, since $U(\mathfrak{m})$ is generated by \mathfrak{m} , then $\mathcal{D}(U(\mathfrak{m}))$ is generated by $\{L_a, R_a \mid a \in \mathfrak{m}\}$. The images of these generators under $\bar{\varphi}$ are $\bar{\varphi}(L_a) = \bar{\varphi}(\rho(P_a)) = \rho(\bar{\varphi}(P_a)) = -\rho(T_a) = \lambda_a$ and $\bar{\varphi}(R_a) = \rho_a$.

The identities that define $\mathcal{D}(U(\mathfrak{m}))$ also imply that

$$\begin{aligned} -L_{ab} &= P_a L_b + L_b R_a = -L_a L_b - [R_a, L_b] \\ -L_{ab} &= R_b L_a + L_a P_b = -L_a L_b - [L_a, R_b] \end{aligned}$$

so $[L_a, R_b] = [R_a, L_b]$ and $[L_a, L_b] = L_{[a, b]} - 2[L_a, R_b]$. In a similar way $[R_a, R_b] = -R_{[a, b]} - 2[L_a, R_b]$. This proves that the generators $\{L_a, R_a \mid a \in \mathfrak{m}\}$ satisfy similar relations to those in (5.1). Therefore, there exists a homomorphism of Hopf algebras $U(\mathcal{L}(\mathfrak{m})) \rightarrow \mathcal{D}(U(\mathfrak{m}))$ that sends λ_a to L_a and ρ_a to R_a . This homomorphism is clearly the inverse of $\bar{\varphi}$, so $\bar{\varphi}$ is an isomorphism of Hopf algebras. \square

6. MOUFANG LOOPS FROM COALGEBRAS MORPHISMS

Let $(\mathcal{C}, \Delta, \epsilon)$ be a cocommutative coalgebra and U a Moufang-Hopf algebra that will remain fixed throughout this section. It is known [13] that the set of coalgebra morphisms $\text{Coalg}(\mathcal{C}, U)$ from \mathcal{C} to U is a Moufang loop with the convolution product $f * g$ given by

$$c(f * g) = \sum (c_{(1)}f)(c_{(2)}g),$$

the unit element being $c \mapsto \epsilon(c)1$. (Recall, here we have reverted to writing operators on the right as in Section 2.) This is a nonassociative analog of the fact that for any Hopf algebra H , $\text{Coalg}(\mathcal{C}, H)$ is a group under the convolution.

In the vector space $\text{Hom}(\mathcal{C}, \text{End}(U))$ we may also define a convolution product

$$(A * B)_c = \sum A_{c_{(1)}} B_{c_{(2)}}$$

for which $\text{Hom}(\mathcal{C}, \text{End}(U))$ is an associative algebra with identity $c \mapsto \epsilon(c)\text{Id}_U$. The notation for the image A_c of c under A is consistent with the notation L_x, R_x for the multiplication operators on U that we can interpret as elements $L, R \in \text{Hom}(U, \text{End}(U))$. Consider the elements $A \in \text{Hom}(\mathcal{C}, \text{End}(U))$ such that

- (1) A is invertible,
- (2) $\epsilon(yA_x) = \epsilon(y)\epsilon(x)$ and
- (3) $\Delta(yA_x) = \sum y_{(1)}A_{x_{(1)}} \otimes y_{(2)}A_{x_{(2)}}$

and call $G = G(\mathcal{C}, U)$ the set of all of them. Clearly G is a group. For instance, if $\mathcal{C} = U$ then $L: x \mapsto L_x, R: x \mapsto R_x$ belong to $G(U, U)$. In fact,

$$\begin{aligned} \sum yL_{x_{(1)}}L_{x_{(2)}}S &= \epsilon(x)y = \sum yL_{x_{(1)}}SL_{x_{(2)}} \quad \text{and} \\ \sum yR_{x_{(1)}}R_{x_{(2)}}S &= \epsilon(x)y = \sum yR_{x_{(1)}}SR_{x_{(2)}} \end{aligned}$$

show that L and R are invertible in $\text{Hom}(U, \text{End}(U))$ with inverses

$$L^{-1}: x \mapsto L_{xS} \quad \text{and} \quad R^{-1}: x \mapsto R_{xS}.$$

The map $U = L * R: x \mapsto \sum L_{x_{(1)}}R_{x_{(2)}}$ also belongs to $G(U, U)$.

Let us define now

$$\text{Atp}_{\mathcal{C}}(U) = \{(A, B, C) \in G^3 \mid (xy)A_c = \sum (xB_{c_{(1)}})(yC_{c_{(2)}}) \quad \forall x, y \in U, c \in \mathcal{C}\}.$$

To justify our notation observe that when $U = FQ$ is the loop algebra of a Moufang loop Q and $\mathcal{C} = Fe$ is the one-dimensional coalgebra with $\Delta(e) = e \otimes e$ and $\epsilon(e) = 1$, then G can be identified with $\text{Bij}(Q)$ and $\text{Atp}_{\mathcal{C}}(U)$ with $\text{Atp}(Q)$.

The goal of this section is to prove that, in analogy with results in Section 2, $\text{Atp}_{\mathcal{C}}(U)$ is a group with triality for which $\mathcal{M}(\text{Atp}_{\mathcal{C}}(U)) = \text{Coalg}(\mathcal{C}, U)$.

Proposition 6.1. *$\text{Atp}_{\mathcal{C}}(U)$ is a group under the componentwise product.*

Proof. It is easy to check that $\text{Atp}_{\mathcal{C}}(U)$ is closed under products, so we only have to prove that $(A^{-1}, B^{-1}, C^{-1}) \in \text{Atp}_{\mathcal{C}}(U)$ whenever $(A, B, C) \in \text{Atp}_{\mathcal{C}}(U)$. Let $(A, B, C) \in \text{Atp}_{\mathcal{C}}(U)$. On the one hand,

$$\sum (((xB_{c_{(1)}}^{-1})(yC_{c_{(2)}}^{-1}))A_{c_{(3)}})A_{c_{(4)}}^{-1} = \sum (xB_{c_{(1)}}^{-1})(yC_{c_{(2)}}^{-1});$$

while on the other

$$\begin{aligned} \sum (((xB_{c_{(1)}}^{-1})(yC_{c_{(2)}}^{-1}))A_{c_{(3)}})A_{c_{(4)}}^{-1} &= \sum (((xB_{c_{(1)}}^{-1})B_{c_{(2)}})(yC_{c_{(3)}}^{-1})C_{c_{(4)}})A_{c_{(5)}}^{-1} \\ &= (xy)A_c^{-1}. \end{aligned}$$

□

Given $A \in G$ consider

$$L_A: c \mapsto L_{1A_c}, \quad R_A: c \mapsto R_{1A_c}, \quad U_A: c \mapsto U_{1A_c}$$

where $yU_x = \sum x_{(1)}yx_{(2)}$ for any $x, y \in U$. These maps are invertible with inverses

$$(L_A)^{-1} = (L^{-1})_A, \quad (R_A)^{-1} = (R^{-1})_A, \quad \text{and} \quad (U_A)^{-1} = (U^{-1})_A.$$

In fact, $L_A, R_A, U_A \in G(\mathcal{C}, U)$.

Lemma 6.2. *For any $A \in G(\mathcal{C}, U)$ we have that*

$$(L_A, U_A, L_A^{-1}), (R_A, R_A^{-1}, U_A), (U_A, L_A, R_A) \in \text{Atp}_{\mathcal{C}}(U).$$

Proof. This statement is a consequence of the Moufang-Hopf identities. For instance, the left Moufang-Hopf identity implies that

$$(xy)(L_A)_c = \sum (xy)L_{1A_c} = \sum (xU_{1A_{c_{(1)}}})(yL_{1A_{c_{(2)}}}S) = \sum (x(U_A)_{c_{(1)}})(y(L_A^{-1})_{c_{(2)}}).$$

hence $(L_A, U_A, L_A^{-1}) \in \text{Atp}_{\mathcal{C}}(U)$. □

We leave the proof of the following lemma as an exercise.

Lemma 6.3. *Let $B \in G(\mathcal{C}, U)$ be such that $1B_c = \epsilon(c)1$ for any $c \in \mathcal{C}$. Then $L_B = R_B = U_B = 1_{G(\mathcal{C}, U)}$.*

Lemma 6.4. *If $(A, B, C) \in \text{Atp}_{\mathcal{C}}(U)$, then $A = B * R_C$ and $A = C * L_B$. In particular, if $1B_c = \epsilon(c)1$ for all $c \in \mathcal{C}$ then $A = C$.*

Proof. Since $(xy)A_c = \sum (xB_{c_{(1)}})(yC_{c_{(2)}})$, then evaluating at $y = 1$ we obtain $xA_c = \sum (xB_{c_{(1)}})(1C_{c_{(2)}}) = (xB_{c_{(1)}})R_{1C_{c_{(2)}}} = x(B * R_C)_c$. The other equality in the statement follows from evaluating at $x = 1$. □

Lemma 6.5. *Any $(A, B, C) \in \text{Atp}_{\mathcal{C}}(U)$ can be written as*

$$(A, B, C) = (D', D, D')(R_B^{-1}, R_B, U_B^{-1})$$

for some $(D', D, D') \in \text{Atp}_{\mathcal{C}}(U)$.

Proof. The only possibility for (D', D, D') is $(A * R_B, B * R_B^{-1}, C * U_B)$ once we have demonstrated that $A * R_B = C * U_B$; but this relation is a consequence of $1(B * R_B^{-1})_c = \sum (1B_{c_{(1)}})((1B_{c_{(2)}})S) = \epsilon(c)1$ and Lemma 6.4. □

Given $A \in G(\mathcal{C}, U)$ consider

$$A^S: c \mapsto SA_cS.$$

This map is invertible with inverse $(A^{-1})^S$:

$$((A^{-1})^S * A^S)_c = \sum SA_{c_{(1)}}^{-1}SSA_{c_{(2)}}S = \epsilon(c)\text{Id}_U = (A^S * (A^{-1})^S)_c.$$

In fact, it can be easily seen that $A^S \in G(\mathcal{C}, U)$ and that $A \mapsto A^S$ is an involutive automorphism of $G(\mathcal{C}, U)$. In the following we will write A^{-S} instead of $(A^{-1})^S$.

Proposition 6.6. *Let U be a cocommutative Moufang-Hopf algebra and \mathcal{C} a cocommutative coalgebra. Then $\text{Atp}_{\mathcal{C}}(U)$ is a group with triality relative to the automorphisms ρ, σ given by*

$$(A, B, C)^\rho = (B^S, C, A^S) \quad \text{and} \quad (A, B, C)^\sigma = (C, B^S, A)$$

for any $(A, B, C) \in \text{Atp}_{\mathcal{C}}(U)$.

Proof. We can compute $\sum((x_{(1)}S)B_{c_{(1)}}S)((x_{(2)}S)(x_{(3)}y))A_{c_{(2)}})$ either as

$$\sum(xSB_{c_{(1)}}S)(yA_{c_{(2)}})$$

or as

$$\sum(x_{(1)}SB_{c_{(1)}}S)((x_{(2)}SB_{c_{(2)}})((x_{(3)}y)C_{c_{(3)}})) = (xy)C_c.$$

This proves that $(C, B^S, A) \in \text{Atp}_{\mathcal{C}}(U)$. A similar computation for

$$\sum((xy_{(1)})(y_{(2)}S))A_{c_{(1)}}(y_{(3)}SC_{c_{(2)}}S)$$

gives $(B, A, C^S) \in \text{Atp}_{\mathcal{C}}(U)$. Starting with (C, B^S, A) instead of (A, B, C) we get $(B^S, C, A^S) \in \text{Atp}_{\mathcal{C}}(U)$. The maps $\rho: (A, B, C) \mapsto (B^S, C, A^S)$ and $\sigma: (A, B, C) \mapsto (C, B^S, A)$ so defined verify the relations $\sigma^2 = \text{Id}_{\text{Atp}_{\mathcal{C}}(U)} = \rho^3$, $\sigma\rho = \rho^2\sigma$.

At this point we should observe that if $(A, B, A) \in \text{Atp}_{\mathcal{C}}(U)$, then $(A, B^S, A) = (A, B, A)^\sigma \in \text{Atp}_{\mathcal{C}}(U)$ so $(1_{G(\mathcal{C}, U)}, B^{-1} * B^S, 1_{G(\mathcal{C}, U)}) \in \text{Atp}_{\mathcal{C}}(U)$, i.e., $B^{-1} * B^S = 1_{G(\mathcal{C}, U)}$. Therefore $B^S = B$.

The proof of relation (1.3) for $\text{Atp}_{\mathcal{C}}(U)$ is similar to that of Theorem 2.2. The equalities to be checked here are

$$\begin{aligned} A^{-1} * C * B^{-S} * B * C^{-S} * A^S &= 1_{G(\mathcal{C}, U)}, \\ B^{-1} * B^S * C^{-1} * A * A^{-S} * C^S &= 1_{G(\mathcal{C}, U)} \text{ and} \\ C^{-1} * A * A^{-S} * C^S * B^{-1} * B^S &= 1_{G(\mathcal{C}, U)}. \end{aligned}$$

We will only prove the first one. By Lemma 6.4 we can write $A = C * L_B$ so $A^{-1} * C * B^{-S} * B * C^{-S} * A^S = L_B^{-1} * B^{-S} * B * L_B^S$. Now by Lemma 6.5 we decompose (A, B, C) as $(D', D, D')(R_B^{-1}, R_B, U_B^{-1})$ to obtain that $B = D * R_B$ with $D^S = D$. Thus, $A^{-1} * C * B^{-S} * B * C^{-S} * A^S = L_B^{-1} * B^{-S} * B * L_B^S = L_B^{-1} * R_B^{-S} * R_B * L_B^S = 1_{G(\mathcal{C}, U)}$ since $L_B^S = R_B^{-1}$. \square

The loop $\mathcal{M}(\text{Atp}(\mathcal{C}, U))$ consists of the elements

$$(A, B, C)^{-1}(A, B, C)^\sigma = (A^{-1} * C, B^{-1} * B^S, C^{-1} * A) = (L_B^{-1}, U_B^{-1}, L_B).$$

In fact, for any $B \in G(\mathcal{C}, U)$ we have that $(U_B, L_B, R_B) \in \text{Atp}(\mathcal{C}, U)$ and $L_{L_B} = L_B$, so we can identify $\mathcal{M}(\text{Atp}(\mathcal{C}, U))$ with $\{L_B \mid B \in G(\mathcal{C}, U)\}$. The product on $\text{Atp}(\mathcal{C}, U)$ is given by

$$\begin{aligned} (L_B^{-1}, U_B^{-1}, L_B) \cdot (L_{B'}^{-1}, U_{B'}^{-1}, L_{B'}) &= (L_B, U_B, L_B^{-1})^\rho (L_{B'}^{-1}, U_{B'}^{-1}, L_{B'}) (L_B, U_B, L_B^{-1})^{\rho^2} \\ &= (U_B^S, L_B^{-1}, L_B^S) (L_{B'}^{-1}, U_{B'}^{-1}, L_{B'}) (L_B^{-S}, L_B^S, U_B) \\ &= (U_B^{-1}, L_B^{-1}, R_B^{-1}) (L_{B'}^{-1}, U_{B'}^{-1}, L_{B'}) (R_B, R_B^{-1}, U_B) \\ &= (U_B^{-1} * L_{B'}^{-1} * R_B, L_B^{-1} * U_{B'}^{-1} * R_B^{-1}, R_B^{-1} * L_{B'} * U_B). \end{aligned}$$

By the middle Moufang-Hopf identity, the last component $R_B^{-1} * L_{B'} * U_B$ of this triple acts by

$$x(R_B^{-1} * L_{B'} * U_B)_c = \sum((1B_{c_{(1)}})(1B'_{c_{(1)}}))x$$

so, under the identification of $\mathcal{M}(\text{Atp}(\mathcal{C}, U))$ with $\{L_B \mid B \in G(\mathcal{C}, U)\}$, the product is given by

$$L_B \cdot L_{B'} = L_{L_B * R_{B'}}.$$

Proposition 6.7. $\mathcal{M}(\text{Atp}(\mathcal{C}, U))$ and $\text{Coalg}(\mathcal{C}, U)$ are isomorphic Moufang loops.

Proof. Given a coalgebra morphism $\theta: \mathcal{C} \rightarrow U$, define $L_\theta: \mathcal{C} \rightarrow \text{End}(U)$ by $L_\theta: c \mapsto L_{c\theta}$. Since $L_\theta = L_{\theta'}$ if and only if $\theta = \theta'$, we can identify $\text{Coalg}(\mathcal{C}, U)$ with $\{L_\theta \mid \theta \in \text{Coalg}(\mathcal{C}, U)\}$.

The elements L_θ with $\theta \in \text{Coalg}(\mathcal{C}, U)$ belong to $G(\mathcal{C}, U)$, and they also satisfy $L_{L_\theta} = L_\theta$ since $(L_{L_\theta})_c = L_{1(L_\theta)_c} = L_{c\theta} = (L_\theta)_c$. Hence, $\{L_\theta \mid \theta \in \text{Coalg}(\mathcal{C}, U)\} \subseteq \{L_B \mid B \in G(\mathcal{C}, U)\}$. The other inclusion also holds. Given $B \in G(\mathcal{C}, U)$, define θ by $c\theta = 1B_c$. Then $L_\theta = L_B$. The product on $\{L_\theta \mid \theta \in \text{Coalg}(\mathcal{C}, U)\}$ is

$$\begin{aligned} x(L_\theta \cdot L_{\theta'})_c &= x(L_{L_\theta} \cdot L_{L_{\theta'}})_c = \sum ((1(L_\theta)_{c(1)})(1(L_{\theta'})_{c(2)}))x = \sum (\theta_{c(1)}\theta'_{c(2)})x \\ &= x(L_{\theta*\theta'})_c. \end{aligned}$$

Consequently the Moufang loop $\text{Coalg}(\mathcal{C}, U)$ is isomorphic to $\mathcal{M}(\text{Atp}_{\mathcal{C}}(U))$. \square

REFERENCES

- [1] Richard Hubert Bruck, *A survey of binary systems*, Ergebnisse der Mathematik und ihrer Grenzgebiete. Neue Folge, Heft 20. Reihe: Gruppentheorie, Springer Verlag, Berlin, 1958. MR0093552 (20 #76)
- [2] Stephen Doro, *Simple Moufang loops*, Math. Proc. Cambridge Philos. Soc. **83** (1978), no. 3, 377–392. MR0492031 (58 #11195)
- [3] S. M. Gagola III and J. I. Hall, *Lagrange’s theorem for Moufang loops*, Acta Sci. Math. (Szeged) **71** (2005), no. 1–2, 45–64. MR2160355 (2006f:20079)
- [4] George Glauberman, *On loops of odd order. II*, J. Algebra **8** (1968), 393–414. MR0222198 (36 #5250)
- [5] Alexander Grishkov, *Lie algebras with triality*, J. Algebra **266** (2003), no. 2, 698–722. MR1995132 (2004h:17019)
- [6] Alexander N. Grishkov and Andrei V. Zavarnitsine, *Lagrange’s theorem for Moufang loops*, Math. Proc. Cambridge Philos. Soc. **139** (2005), no. 1, 41–57. MR2155504 (2006d:20122)
- [7] ———, *Groups with triality*, J. Algebra Appl. **5** (2006), no. 4, 441–463. MR2239539 (2007g:20062)
- [8] ———, *Sylow’s theorem for Moufang loops*, J. Algebra **321** (2009), no. 7, 1813–1825. MR2494749 (2010h:20159)
- [9] Jonathan I. Hall, *On Mikheev’s construction of enveloping groups*, Comment. Math. Univ. Carolin. **51** (2010), no. 2, 245–252.
- [10] ———, *Moufang loops and groups with triality are essentially the same thing*, submitted.
- [11] P. O. Mikheev, *On the embedding of Mal’tsev algebras into Lie algebras*, Algebra i Logika **31** (1992), no. 2, 167–173, 221 (Russian, with Russian summary); English transl., Algebra and Logic **31** (1992), no. 2, 106–110 (1993). MR1289030
- [12] ———, *Groups that envelop Moufang loops*, Uspekhi Mat. Nauk **48** (1993), no. 2(290), 191–192 (Russian, with Russian summary); English transl., Russian Math. Surveys **48** (1993), no. 2, 195–196. MR1239875 (94g:20098)
- [13] José M. Pérez-Izquierdo, *Algebras, hyperalgebras, nonassociative bialgebras and loops*, Adv. Math. **208** (2007), no. 2, 834–876. MR2304338 (2008f:17006)
- [14] José M. Pérez-Izquierdo and Ivan P. Shestakov, *An envelope for Malcev algebras*, J. Algebra **272** (2004), no. 1, 379–393. MR2029038 (2004j:17040)
- [15] Hala O. Pflugfelder, *Quasigroups and loops: introduction*, Sigma Series in Pure Mathematics, vol. 7, Heldermann Verlag, Berlin, 1990. MR1125767 (93g:20132)
- [16] Richard D. Schafer, *An introduction to nonassociative algebras*, Dover Publications Inc., New York, 1995. Corrected reprint of the 1966 original. MR1375235 (96j:17001)
- [17] Jonathan D. H. Smith and Anna B. Romanowska, *Post-modern algebra*, Pure and Applied Mathematics (New York), John Wiley & Sons Inc., New York, 1999. A Wiley-Interscience Publication. MR1673047 (2000d:00001)
- [18] K. A. Zhevlakov, A. M. Slin’ko, I. P. Shestakov, and A. I. Shirshov, *Rings that are nearly associative*, Pure and Applied Mathematics, vol. 104, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], New York, 1982. Translated from the Russian by Harry F. Smith. MR668355 (83i:17001)

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WISCONSIN, MADISON, WISCONSIN 53706 USA
E-mail address: `benkart@math.wisc.edu`

DPTO. MATEMÁTICAS Y COMPUTACIÓN, UNIVERSIDAD DE LA RIOJA, 26006, LOGROÑO, ESPAÑA
E-mail address: `sara.madariaga@unirioja.es`

DPTO. MATEMÁTICAS Y COMPUTACIÓN, UNIVERSIDAD DE LA RIOJA, 26006, LOGROÑO, ESPAÑA
E-mail address: `jm.perez@unirioja.es`